TIGR Threat Bulletin

SecurityRisk ADVISORS

Microsoft Patch Tuesday

July 11, 2023

Executive Summary

The Microsoft Security Response Center (MSRC) reported 132 vulnerabilities across many Windows and Microsoft products, features, and roles. Of the 132 patched bugs, nine (9) are classified as critical severity and six (6) are being actively exploited. The number of bugs in each category is listed below:

- 33 Elevation of Privilege
- 13 Security Feature Bypass
- 37 Remote Code Execution (RCE)
- 19 Information Disclosure
- 22 Denial of Service (DoS)
- 7 Spoofing

Featured Critical Vulnerabilities

The six (6) actively exploited vulnerabilities listed in July's Patch Tuesday security update are listed below.

Windows MSHTML	Windows SmartScreen	Windows Error Reporting Service	Office and Windows HTML
CVE-2023-32046	CVE-2023-32049	CVE-2023-36874	CVE-2023-36884
Microsoft Signed Drivers	**Microsoft Outlook**		
ADV230001	CVE-2023-35311		

Safeguards/Recommendations

Organizations should ensure all systems, software, data, and device settings are backed up prior to performing updates and security patches. Users can regularly monitor the "Check for Updates" in their Windows device settings to ensure systems are up-to-date with the latest security patches. For a full list of affected products, features, and roles, visit MSRC's July 2023 Patch Tuesday release notes.

References

- https://msrc.microsoft.com/update-guide/releaseNote/2023-Jul
- https://msrc.microsoft.com/update-guide/